(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 779 599**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 07026**

(51) Int Cl⁶ : H 04 N 7/16, H 03 M 13/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 04.06.98.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 10.12.99 Bulletin 99/49.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *DASSAULT AUTOMATISMES ET TELECOMMUNICATIONS Société anonyme* — FR.

(72) Inventeur(s) : BASSET JEAN CLAUDE.

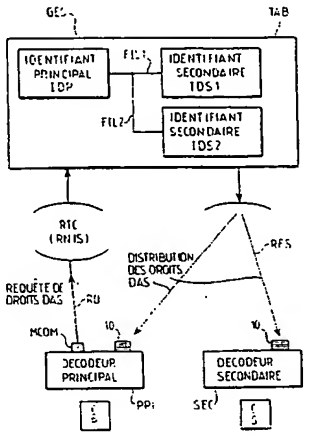
(73) Titulaire(s) :

(74) Mandataire(s) : CABINET NETTER.

(54) DISPOSITIF DE TELEVISION A PEAGE EQUIPE DE PLUSIEURS DECODEURS AVEC DISTRIBUTION DE DROITS D'ACCES.

(57) Le dispositif de télévision à péage coopère avec au moins un réseau de diffusion (RES) et un centre de gestion de droits d'accès (GES). Il comprend un décodeur principal (PRI) et un décodeur secondaire (SEC) apte chacun à procéder à la conversion de signaux embrouillés en provenance du réseau de diffusion en des signaux désembrouillés. Chaque décodeur comprend un module de contrôle d'accès coopérant avec une carte à mémoire (55) contenant un identifiant d'usager, associé à des droits d'accès.

Des moyens de communication (MCOM) relient le décodeur principal au centre de gestion (GES) pour requérir les droits d'accès secondaires (DAS), en fonction de l'identifiant d'usager principal, de l'identifiant d'usager secondaire et d'une information de filiation, et pour recevoir lesdits droits d'accès secondaires ainsi requis, au niveau du décodeur principal (PRI) ou du décodeur secondaire (SEC), via le réseau de diffusion (RES) en vue d'être transférés dans la carte secondaire (CS).



FR 2 779 599 - A1

Dispositif de télévision à péage équipé de plusieurs décodeurs avec distribution de droits d'accès.

La présente invention concerne les services et/ou communications à péage, notamment la télévision.

Elle trouve une application dans les réseaux de diffusion hertzienne, directe par satellite ou par câble, dans lesquels les informations diffusées (son, image et parfois données) sont "embrouillées", c'est-à-dire modifiées selon un codage spécifique, pour interdire l'accès à ces informations. Un désembrouilleur ou décodeur, loué ou vendu aux usagers pour un usage bien délimité, leur permet d'accéder aux informations "désembrouillées", c'est-à-dire en clair.

D'une manière générale, lorsqu'on possède plusieurs récepteurs de télévision et qu'on souhaite recevoir des émissions de télévision à péage sur chacun des récepteurs de télévision, on doit relier un décodeur à chaque récepteur, et on doit obtenir des droits d'accès individuels pour chaque décodeur.

Toutefois, les décodeurs sont relativement coûteux à l'achat ou à la location, et la procédure d'obtention des droits d'accès auprès d'un opérateur est relativement lourde à mettre en place et peu flexible, notamment lorsqu'il y a plusieurs usagers à satisfaire avec des besoins différents.

La présente invention apporte une solution à ces problèmes.

Elle porte sur un dispositif de télévision à péage destiné à coopérer avec au moins un réseau de diffusion et un centre de gestion de droits d'accès, ledit dispositif de télévision étant du type comprenant un décodeur principal apte à procéder à la conversion de signaux embrouillés portant des informations sujettes à péage en provenance du réseau de diffusion en des signaux désembrouillés, susceptibles d'utilisation directe, ledit décodeur principal comprenant un

module de contrôle d'accès principal apte à coopérer avec une carte à mémoire principale contenant un identifiant d'usager principal, associé à des droits d'accès principaux, et des moyens de communication propres à être reliés au centre de gestion.

Selon une définition générale de l'invention, le dispositif comprend en outre au moins un décodeur secondaire apte à procéder à la conversion des signaux embrouillés en des signaux désembrouillés, ledit décodeur secondaire comprenant un module de contrôle d'accès secondaire apte à coopérer avec au moins une carte à mémoire secondaire contenant un identifiant d'usager secondaire, associé à des droits d'accès secondaires, l'identifiant d'usager secondaire étant relié à l'identifiant d'usager principal selon une information de filiation prédéterminée.

Selon encore la définition générale de l'invention, les moyens de communication du décodeur principal sont propres à dialoguer avec le centre de gestion pour requérir lesdits droits d'accès secondaires, en fonction de l'identifiant d'usager principal, de l'identifiant d'usager secondaire et de l'information de filiation, et le décodeur principal ou le décodeur secondaire est propre à recevoir, via le réseau de diffusion, lesdits droits secondaires ainsi requis, afin de les transférer dans la carte à mémoire secondaire.

Un tel dispositif a l'avantage de permettre d'obtenir des droits d'accès pour la ou les cartes à mémoire associées à chaque décodeur, à l'aide d'un dialogue entre les moyens de communication du décodeur équipé de tels moyens de communication et le centre de gestion, les autres décodeurs pouvant être des décodeurs dépourvus de moyens de communication avec le centre de gestion et simplement dédiés à la conversion des signaux embrouillés.

Il en résulte qu'un tel dispositif est plus ergonomique et moins coûteux qu'un dispositif comprenant des décodeurs équipés chacun de moyens de communication avec le centre de

gestion. En outre, un tel dispositif selon l'invention simplifie la distribution des droits d'accès pour une ou plusieurs cartes à mémoires secondaires associées à un ou plusieurs décodeurs secondaires.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lumière de la description détaillée ci-après et des dessins dans lesquels :

- la figure 1 représente schématiquement le principe de fonctionnement d'un système de télévision à péage de l'art antérieur ;

- la figure 2 est un schéma détaillé de la distribution des droits d'accès aux émissions de télévision selon l'art antérieur ;

- la figure 3 représente schématiquement un mode de réalisation de l'invention ; et

- la figure 4 est un organigramme illustrant la distribution des droits d'accès secondaires selon l'invention.

Sur la figure 1, un décodeur DEC comprend une interface d'entrée 10 qui reçoit un signal analogique ou numérique embrouillé qui peut être par exemple :

- soit un signal analogique haute fréquence comprenant plusieurs canaux de données, auquel cas l'interface d'entrée 10 comporte alors un démodulateur, pour passer en fréquence plus basse, et un démultiplexeur, pour séparer les canaux individuels ;

- soit directement un signal analogique embrouillé concernant un seul canal, auquel cas l'interface d'entrée 10 comprend simplement des éléments de mise en forme de ce signal ;

- soit un signal numérique porteur du flux numérique, et [illegible] d'entrée 10 peut être soit un récepteur/syn-

toniseur (tuner) de télévision par câble ou par satellite, soit un coupleur de type ATM (mode de transfert asynchrone ou "Asynchronus Transfer Mode"), ou encore ADSL (Ligne d'abonné numérique asymétrique ou "Asymetric Digital Subscriber Line").

De façon connue, des moyens de traitement 20 sont capables de transformer les signaux embrouillés d'un seul canal en signaux désembrouillés, qui sont alors appliqués à l'interface de sortie 90, pour commander par exemple un téléviseur ou un moniteur, dans le cas d'une application vidéo.

L'interface de sortie 90 dans le cas d'un signal numérique peut comprendre un démultiplexeur, pour extraire du flux numérique en clair les séquences relatives au canal souhaité, et l'interface de sortie proprement dite, qui, de façon connue, transforme ces séquences en signaux propres à piloter un téléviseur ou un moniteur.

Le décodeur DEC comprend en outre des moyens de communication MCOM reliés au centre de gestion des droits d'accès GES. Ces moyens de communication MCOM forment une voie de retour entre le décodeur DEC et le centre de gestion GES.

Par exemple, ces moyens de communication MCOM comprennent un modulateur/démodulateur de type MODEM téléphonique reliant le décodeur au centre de gestion via le réseau téléphonique commuté RTC ou le réseau numérique à intégration de services RNIS.

La voie de retour entre le décodeur et le centre de gestion trouve des applications d'interactivité, par exemple pour demander des droits d'accès ou faciliter la navigation dans les programmes et canaux.

Une télécommande TCOM est associée au décodeur pour permettre à l'usager de sélectionner son programme ou s'informer en permanence et l'aider à faire son choix en consultant une base de données relative aux émissions en cours ou à venir.

En référence à la figure 2, le dispositif embrouilleur 100 reçoit à son entrée 102 les composantes en clair CC à embrouiller. Les informations de synchronisation et de signalisation SSC sont appliquées en clair à l'entrée 104 de l'embrouilleur. La sortie 106 de l'embrouilleur, délivrant les composantes embrouillées CE, est reliée à l'entrée 112 du désembrouilleur 110 dont l'entrée 114 reçoit les informations de synchronisation et de signalisation en clair SSC. Après conversion, la sortie 116 du désembrouilleur délivre les composantes en clair CC.

L'embrouillage/désembrouillage est commandé par un mot de contrôle CW. Le désembrouilleur doit posséder le même mot de contrôle CW que l'embrouilleur pour restituer l'image ou le son en clair.

En pratique, les mots de contrôle CW sont transmis sensiblement en temps réel dans le signal diffusé par le réseau de diffusion RES, sous forme chiffrée pour protéger leur transport depuis l'embrouilleur jusqu'au désembrouilleur.

Côté émission, un dispositif de chiffrement 120 reçoit à son entrée 122 les mots de contrôle CW à chiffrer selon une fonction cryptographique f sous contrôle d'une clé d'autorisation SK, appelée encore clé de service ou service_key, et appliquée à l'entrée 124 du dispositif de chiffrement.

Les cryptogrammes correspondants aux transformés des mots de contrôle CW par la fonction cryptographique f selon la clé d'autorisation SK, c'est-à-dire f(CW,SK), sont transmis par la sortie 128 dans le signal diffusé à l'intérieur de messages de services appelés ECM (Entitlement Control Messages). La sortie 126 applique les mots de contrôle CW en clair à l'entrée 105 de l'embrouilleur 100.

Les messages de service ECM comprennent en outre les conditions d'accès CA au programme (coût, type d'abonnement, etc) appliquées à l'entrée 130 du dispositif de chiffrement 120.

Toutes les informations contenues dans les messages de service ECM sont signées par le dispositif de chiffrement 120 à l'aide de la clé d'autorisation SK. La sortie 128 applique au signal diffusé par le réseau de diffusion lesdites informations signées correspondants à f(ECM,SK).

Au niveau de chaque décodeur DEC, les messages de service ECM du programme sélectionné par l'usager sont récupérés et la signature f(ECM,SK) est vérifiée. En présence d'une signature authentique et si les conditions d'accès CA sont satisfaites, les mots de contrôle CW sont alors déchiffrés et transmis au désembrouilleur 110, c'est-à-dire aux moyens de traitement 20 du décodeur DEC décrit en référence à la figure 1.

La vérification de la signature de f(ECM,SK) et le déchiffrement de f(CW,SK) se font grâce à un dispositif de déchiffrement 200 utilisant la même clé d'autorisation SK qu'à l'émission. L'entrée 202 du dispositif de déchiffrement 200 reçoit les transformés f(ECM,SK) et f(CW,SK) via le réseau de diffusion. L'entrée 204 du dispositif de déchiffrement 200 reçoit la clé SK. La sortie 206 du dispositif de déchiffrement 200 délivre les mots de contrôle CW à l'entrée 118 du désembrouilleur 110.

Le dispositif de déchiffrement 200 ainsi que la clé d'autorisation SK sont stockés dans un module de contrôle d'accès 50 (figure 1) qui, lui-même, coopère avec une mémoire protégée 55 (figure 1).

La mémoire 55 peut être par exemple une carte à puce à microprocesseur, ou bien une clé électronique à microprocesseur, ou bien une carte de type PCMCIA avec processeur sécurisé, ou encore une carte sans contact sécurisée à microprocesseur.

La clé d'autorisation SK n'est pas diversifiée, c'est-à-dire que la même clé d'autorisation SK est présente dans toutes les cartes d'accès.

Un dispositif comparateur 210 est prévu pour comparer les droits d'accès DA aux conditions d'accès à un programme CA transmises dans les messages de services ECM afin d'établir si l'usager a le droit ou non de regarder le programme.

La mise à jour de ces droits d'accès DA se fait au moyen de messages de gestion des droits d'accès, appelés EMM (Entitlement Management Messages) transmis avec le programme via le réseau.

En pratique, la clé SK est transmise dans le signal diffusé par le réseau de diffusion RES, sous forme chiffrée pour protéger son transport depuis l'embrouilleur jusqu'au désembrouilleur.

Côté émission, un dispositif de chiffrement 220 reçoit à son entrée 222 la clé SK à chiffrer selon une fonction cryptographique f sous contrôle d'une clé de distribution, appelée clé d'utilisateur ou user_key UK. Ces clés de distribution UK varient d'une carte d'accès à une autre. Les clés UK sont appliquées à l'entrée 224 du dispositif de chiffrement 220.

Le transformé de la clé SK par la fonction cryptographique f selon la clé de distribution UK, c'est-à-dire f(SK,UK), est transmis par la sortie 228 dans le signal diffusé à l'intérieur des messages EMM.

Les messages de service EMM comprennent en outre les droits d'accès DA associés à l'usager détenteur de la clé de distribution UK. Ces droits d'accès DA sont appliqués à l'entrée 230 du dispositif de chiffrement 220. En pratique, ces droits d'accès DA sont stockés dans une table TAB logée dans le centre de gestion GES, à une adresse prédéterminée reliant l'identifiant ID de la carte d'accès et lesdits droits d'accès. A chaque identifiant ID sont associés des droits d'accès DA, ainsi qu'une clé de distribution UK.

Toutes les informations (notamment les droits DA) contenues dans les messages de service EMM sont signées par le dispositif de chiffrement 220 à l'aide de la clé de distribution UK.

La sortie 228 applique au signal diffusé par le réseau de diffusion lesdites informations signées correspondant à f(EMM,UK).

Au niveau de chaque décodeur DEC, les messages de gestion de droits d'accès EMM sont récupérés et la signature f(EMM,UK) est vérifiée. En présence d'une signature authentique, la clé d'autorisation SK est alors déchiffrée et transmise à l'entrée 204 du dispositif de déchiffrement 200.

La vérification de la signature de f(EMM,UK) et le déchiffrement de f(SK,UK) se font grâce à un dispositif de déchiffrement 300 utilisant la clé de distribution UK, préalablement stockée dans la mémoire 55 du module de contrôle d'accès.

L'entrée 302 du dispositif de déchiffrement 300 reçoit les transformés f(EMM,UK) et f(SK,UK) via le réseau de diffusion. L'entrée 304 du dispositif de déchiffrement 300 reçoit la clé UK. La sortie 306 du dispositif de déchiffrement 300 délivre la clé SK à l'entrée 204 du dispositif de déchiffrement 200.

Le dispositif de déchiffrement 300 ainsi que la clé de distribution UK sont stockés dans le module de contrôle d'accès 50 (figure 1) et sa mémoire 55.

Les clés de distribution UK varient d'un module de contrôle d'accès à un autre. Elles sont diversifiées au niveau d'un dispositif de génération 400 dont l'entrée 402 reçoit une clé maîtresse participant à la diversification des clés de distribution UK et dont l'entrée 404 reçoit des informations relatives aux fichiers des usagers et des cartes d'accès et contenues dans la table TAB logée dans le centre de gestion GES.

Si la signature des messages EMM est correcte, alors le module de contrôle d'accès, convaincu de l'authenticité du message, exécute l'opération de gestion des droits d'accès après stockage des droits d'accès dans une mémoire 310 dont la sortie 312 est reliée à l'entrée 212 du comparateur de droits 210.

La Demanderesse s'est posé notamment le problème d'améliorer la procédure de distribution des droits d'accès lorsqu'un ou plusieurs usagers possèdent plusieurs récepteurs de télévision reliés chacun à un décodeur.

En référence à la figure 3, on a représenté une installation de télévision à péage équipée d'un décodeur principal PRI et d'un décodeur secondaire SEC.

Le décodeur principal PRI comprend les éléments décrits en référence aux figures 1 et 2, notamment une interface d'entrée 10 recevant les signaux diffusés par le réseau de diffusion RES et des moyens de communication MCOM reliés au centre de gestion GES à travers un réseau de communication quelconque tel que le réseau autocommuté RTC ou le réseau numérique à intégration de services RNIS.

Le décodeur secondaire SEC comprend un désembrouilleur similaire à celui du décodeur principal. Par contre, le décodeur secondaire est avantageusement dépourvu de moyens de communication MCOM, devenus inutiles comme on le verra ci-après. Le décodeur secondaire peut donc être moins cher que le décodeur principal dans la mesure où il n'est pas nécessaire qu'il dispose d'un navigateur pour permettre à l'usager de naviguer dans les programmes et sa télécommande peut avoir des fonctions réduites.

Le module de contrôle d'accès du décodeur secondaire est similaire à celui du décodeur principal. Le module de contrôle d'accès secondaire est apte à coopérer avec une ou plusieurs cartes secondaires CS tandis que le décodeur principal fonctionne avec une carte principale CP.

Selon l'invention, la Demanderesse a mis en place un dialogue entre le décodeur principal et le centre de gestion pour permettre de distribuer des droits d'accès à une ou plusieurs cartes secondaires d'un ou plusieurs décodeurs secondaires sans équiper le ou lesdits décodeurs secondaires de moyens de communication avec le centre de gestion.

Selon l'invention, la table d'identification TAB contient une information de filiation FIL entre l'identifiant de l'usager principal IDP et l'un ou plusieurs identifiants d'accès secondaire IDS.

La gestion des droits d'accès est effectuée selon l'invention à partir de la carte principale. Ainsi, selon l'invention, on peut particulariser ou personnaliser les services offerts par l'opérateur de diffusion aux utilisateurs des décodeurs secondaires qui peuvent utiliser un décodeur secondaire à des instants différents comme des multi-utilisateurs ayant chacun une autorisation personnalisée. Ainsi, un décodeur secondaire peut servir à plusieurs utilisateurs secondaires, ayant chacun une carte secondaire et des droits affectés à ces cartes.

Par exemple, le décodeur principal PRI et la carte principale CP sont affectés à la famille, avec un identifiant principal IDP associé à des droits d'accès DAP pour la famille. Le décodeur secondaire SEC et la ou les cartes secondaires CS1, CS2 sont affectés à des membres de la famille, avec un identifiant secondaire IDS, des droits secondaires DAS et une clé de distribution UK respectifs. Une information de filiation est établie entre les différents identifiants, selon une arborescence choisie et connue du centre de gestion.

Les droits d'accès DAP peuvent être différents des droits d'accès secondaires DAS, et les droits d'accès secondaires de chaque carte secondaire peuvent également être différents les uns des autres.

De plus, le décodeur principal et le ou les décodeurs secondaires ne sont pas nécessairement situés dans le même local. Dans ce cas, le décodeur secondaire est distant du décodeur principal, les droits d'accès secondaires étant cependant liés aux autorisations accordées au moment de l'obtention et stockage desdits droits que l'on décrira plus en détail ci-après.

En référence à la figure 4, on va donner un exemple de distribution de droits d'accès secondaires selon l'invention.

Lorsqu'un usager secondaire veut utiliser un décodeur secondaire pour accéder à des émissions à péage, il est nécessaire de disposer dans sa carte secondaire des droits d'accès correspondants DAS. La carte secondaire CP contient dans sa mémoire protégée une clé de distribution personnelle et secrète UKS.

Selon l'invention, les moyens de communication du décodeur principal vont permettre de dialoguer avec le centre de gestion pour obtenir ces droits d'accès secondaires.

La première étape E1, facultative, consiste à identifier la carte principale CP au niveau du décodeur principal.

Cette identification peut être réalisée à l'aide d'un code personnel secret, introduit au préalable par l'opérateur dans la mémoire secrète de la mémoire, et vérifié par la carte elle-même, à travers le décodeur principal. Une telle identification peut être aménagée pour permettre un fonctionnement multi-utilisateur.

Les étapes E2 et E3 consistent en un dialogue entre le décodeur principal PRI et le centre de gestion GES, via les moyens de communication MCOM.

Selon l'invention, les moyens de communication MCOM émettent une requête RQ auprès du centre de gestion pour obtenir des

droits d'accès secondaires DAS1 (étape E2) pour la ou les cartes secondaires CS.

La requête est accompagnée de l'identifiant d'usager principal IDP, et d'une demande de droits d'accès pour l'identifiant d'usager secondaire IDS. Une information de filiation FIL entre l'identifiant d'usager principal IDP et l'identifiant d'usager secondaire IDS accompagne également la requête.

Avantageusement, la requête est authentifiée selon l'étape E3 à l'aide d'une authentification active mise en place à l'aide de la clé de distribution UK de la carte principale et des moyens de chiffrement 220 logés dans le centre de gestion GES et des moyens de déchiffrement 300 logés au niveau de la carte principale CP.

Après vérification et autorisation, c'est-à-dire authentification de la requête RQ, le centre de gestion va rechercher dans sa table d'identification TAB (étape E4), l'identifiant secondaire IDS. A l'aide de l'information de filiation FIL reliant l'identifiant principal IDP et l'identifiant secondaire IDS, le centre de gestion détermine l'adresse secondaire où se trouvent les droits d'accès secondaires DAS.

Selon l'étape E5, le centre de gestion va attribuer et chiffrer les droits d'accès secondaires DAS pour la carte secondaire CS.

En pratique, les droits d'accès secondaires DAS sont chiffrés par les moyens d'authentification 220 du centre de gestion qui cryptent les droits d'accès secondaires à l'aide de la clé de distribution UKP associée à la carte principale ou à l'aide de la clé de distribution UKS associée à la carte secondaire.

Selon l'étape E6, les droits d'accès secondaires DAS ainsi chiffrés sont transmis via le réseau de diffusion RES vers le décodeur principal ou le décodeur secondaire pour être

déchiffrés et enregistrés dans la carte secondaire (étape E7).

Plus précisément, les moyens de déchiffrement 300 de la carte principale CP ou de la carte secondaire CS établissent la fonction cryptographique f à l'aide de la clé de distribution correspondante pour décrypter les droits d'accès secondaires DAS ainsi transmis cryptés.

En pratique, ce sont les moyens de déchiffrement de la carte principale qui déchiffrent les droits d'accès lorsque le lecteur de carte du décodeur principal comprend deux fentes d'introduction, tandis que ce sont les moyens de déchiffrement de la carte secondaire qui déchiffrent les droits d'accès lorsque le lecteur de carte du décodeur principal ne comprend qu'une seule fente d'introduction.

Dans le cas d'un décodeur principal à deux fentes d'introduction de cartes, la requête RQ est établie lorsque la carte à mémoire principale CP est introduite dans la première fente du décodeur principal et lorsque la carte à mémoire secondaire CS est introduite dans la seconde fente du décodeur principal. Ainsi, les droits secondaires DAS transmis via le réseau de diffusion RES sont d'abord stockés dans la carte à mémoire principale CP pour être ensuite déchiffrés et enfin transférés de la carte à mémoire principale CP vers la carte à mémoire secondaire CS ainsi introduite dans le lecteur de carte principal.

Il est à remarquer que le transfert des droits DAS vers la carte secondaire peut s'effectuer pendant l'utilisation normale du décodeur principal. L'opération de transfert peut s'effectuer en parallèle avec le fonctionnement normal du décodeur principal. L'utilisateur secondaire après retrait de sa carte secondaire dans le décodeur principal peut l'utiliser normalement sur son décodeur secondaire. Il s'agit en fait d'un transfert de droits de type carte principale à carte secondaire.

Dans le cas d'un décodeur principal à une seule fente d'introduction de cartes, la requête RQ est établie lorsque la carte à mémoire principale est introduite dans la fente du décodeur principal et lorsque la carte à mémoire secondaire est introduite dans la fente du décodeur secondaire. Ainsi, les droits secondaires sont transmis directement dans la carte à mémoire secondaire, via le réseau de diffusion selon l'étape E7 pour être déchiffrés et enregistrés.

Dans le cas d'un transfert par le réseau de diffusion directement au niveau de la carte secondaire, la carte principale reste donc dans le décodeur principal et la carte secondaire reste dans le décodeur secondaire.

Enfin, selon l'étape E8, après stockage des droits d'accès secondaires DAS dans la carte secondaire, le désembrouillage et la visualisation du programme sont rendus possibles.

Il est à remarquer que le dialogue décrit ci-avant peut être mis en oeuvre par un dispositif de validation (valideur) de type professionnel situé au niveau d'un point d'accès prédéterminé. Dans ce cas, le décodeur principal PRI, de préférence à deux fentes d'introduction de cartes, décrit en référence aux figures 1 à 4, joue le rôle du valideur d'accès permettant d'effectuer des demandes de droits d'accès REQ auprès du centre de gestion GES de l'opérateur pour une ou plusieurs cartes principale et/ou secondaire, selon le protocole de distribution de droits d'accès conformément à l'invention.

Cette distribution de droits peut être automatisée en libre-service dans une borne spécialisée dans la vente de services opérateurs. Par exemple, la borne spécialisée est apte à assurer l'édition de cartes de pré-paiement, ce qui permet à un décodeur secondaire de donner accès au service lié au pré-paiement sans que ledit décodeur secondaire ne dispose de moyens de communication MCOM avec le centre de gestion GES de l'opérateur.

D'une manière générale, un code parental est à un niveau d'accès à un certain contenu pour un même canal. Selon l'invention, un tel code parental peut être affecté à chaque droits secondaires par le décodeur principal selon une procédure de distribution similaire à celle des droits d'accès secondaires décrite en référence à la figure 4.

Dans ce cas, la carte d'accès principal possède l'image des droits d'accès de toutes les cartes d'accès secondaires et peut autoritairement y affecter un niveau parental. Ce niveau est transmis au décodeur secondaire par le réseau de diffusion dans le cadre d'un message de service. Il peut également être transmis par un transfert carte principale à carte secondaire.

L'opération de transfert d'un code parental peut s'effectuer en vérifiant la carte secondaire par le code personnel affecté à la carte secondaire.

En pratique, le dispositif selon l'invention peut être accompagné de moyens de paiement qui peuvent être une carte bancaire avec accord de crédit et fonctionnant via les moyens de communication MCOM. Les moyens de paiement peuvent être également des moyens externes, par exemple Minitel, borne automatique, commande facture ou serveur spécialisé d'opérateurs par téléphone.

En pratique, les moyens de paiement des droits d'accès principaux et/ou secondaires sont situés dans le décodeur principal.

Revendications

1. Dispositif de télévision à péage destiné à coopérer avec au moins un réseau de diffusion (RES) et un centre de gestion de droits d'accès (GES), ledit dispositif de télévision étant du type comprenant :

- un décodeur principal (PRI) apte à procéder à la conversion de signaux embrouillés portant des informations sujettes à péage en provenance du réseau de diffusion en des signaux désembrouillés, susceptibles d'utilisation directe, ledit décodeur principal comprenant un module de contrôle d'accès principal (50) apte à coopérer avec une carte à mémoire principale (55) contenant un identifiant d'usager principal, associé à des droits d'accès principaux, et

- des moyens de communication (MCOM) propres à être reliés au centre de gestion (GES),

caractérisé en ce qu'il comprend en outre au moins un décodeur secondaire (SEC) apte à procéder à la conversion des signaux embrouillés en des signaux désembrouillés, ledit décodeur secondaire (SEC) comprenant un module de contrôle d'accès secondaire apte à coopérer avec au moins une carte à mémoire secondaire (CS) contenant un identifiant d'usager secondaire (IDS), associé à des droits d'accès secondaires (DAS), l'identifiant d'usager secondaire (IDS) étant relié à l'identifiant d'usager principal selon une information de filiation prédéterminée (FIL), en ce que les moyens de communication (MCOM) sont propres à dialoguer avec le centre de gestion (GES) pour requérir lesdits droits d'accès secondaires (DAS), en fonction de l'identifiant d'usager principal, de l'identifiant d'usager secondaire et de l'information de filiation, et pour recevoir lesdits droits d'accès secondaires ainsi requis, au niveau du décodeur principal (PRI) ou du décodeur secondaire (SEC), via le réseau de diffusion (RES), en vue d'être transférés dans la carte secondaire (CS).

2. Dispositif selon la revendication 1, dans lequel le centre de gestion (GES) comprend des moyens de chiffrement (220) propres à établir une fonction cryptographique (f) à l'aide d'une clé de distribution (UKP), secrète et personnelle à l'usager principal, caractérisé en ce que la carte principale (CP) comprend des moyens de déchiffrement (300) propres à établir la fonction cryptographique (f) à l'aide de la clé de distribution, secrète et personnelle à l'usager principal (UKP), et en ce que les moyens de chiffrement et de déchiffrement (220, et 300) sont propres à authentifier de façon active la requête (RQ) des droits d'accès secondaires (DAS).

3. Dispositif selon la revendication 2, dans lequel les moyens de chiffrement (220) du centre de gestion sont propres à chiffrer les droits d'accès secondaires (DAS), caractérisé en ce que les moyens de déchiffrement (300) de la carte secondaire ou de la carte principale sont propres à déchiffrer les droits d'accès secondaires ainsi transmis chiffrés.

4. Dispositif selon la revendication 1, dans lequel le décodeur principal comprend un lecteur de cartes équipé de premières et secondes fentes, caractérisé en ce que la requête (RQ) est établie lorsque la carte à mémoire principale est introduite dans la première fente et lorsque la carte à mémoire secondaire est introduite dans la seconde fente, et en ce que les droits secondaires sont reçus au niveau du décodeur principal, stockés dans la carte à mémoire principale, et transférés depuis la carte à mémoire principale vers la carte à mémoire secondaire.

5. Dispositif selon la revendication 1, dans lequel le décodeur principal comprend un lecteur de cartes à une seule fente, caractérisé en ce que la requête (RQ) est établie lorsque la carte à mémoire principale est introduite dans la fente du lecteur du décodeur principal et lorsque la carte à mémoire secondaire est introduite dans la fente du lecteur du décodeur secondaire, et en ce que les droits d'accès secon-

daires sont reçus au niveau du décodeur secondaire, et stockés directement dans la carte à mémoire secondaire.

6. Dispositif selon l'une des revendications précédentes, caractérisé en ce que l'utilisateur de la carte principale est propre à créer et affecter des droits de type code parental à l'utilisateur de la carte secondaire selon une procédure de distribution similaire à celle des droits secondaires.

7. Dispositif selon l'une des revendications précédentes, caractérisé en ce que le décodeur principal (PRI) est susceptible d'être un valideur d'accès permettant d'effectuer des demandes de droits d'accès (REQ) auprès du centre de gestion (GES) de l'opérateur pour une ou plusieurs cartes principale et/ou secondaire.

8. Dispositif selon la revendication 7, caractérisé en ce que le valideur d'accès constitue une borne spécialisée dans la vente de services.

9. Dispositif selon la revendication 8, caractérisé en ce que la borne spécialisée est apte à assurer l'édition de cartes de pré-paiement, ce qui permet à un décodeur secondaire (SEC) de donner accès au service lié au pré-paiement sans que ledit décodeur secondaire (SEC) ne dispose de moyens de communication (MCOM) avec le centre de gestion (GES) de l'opérateur.

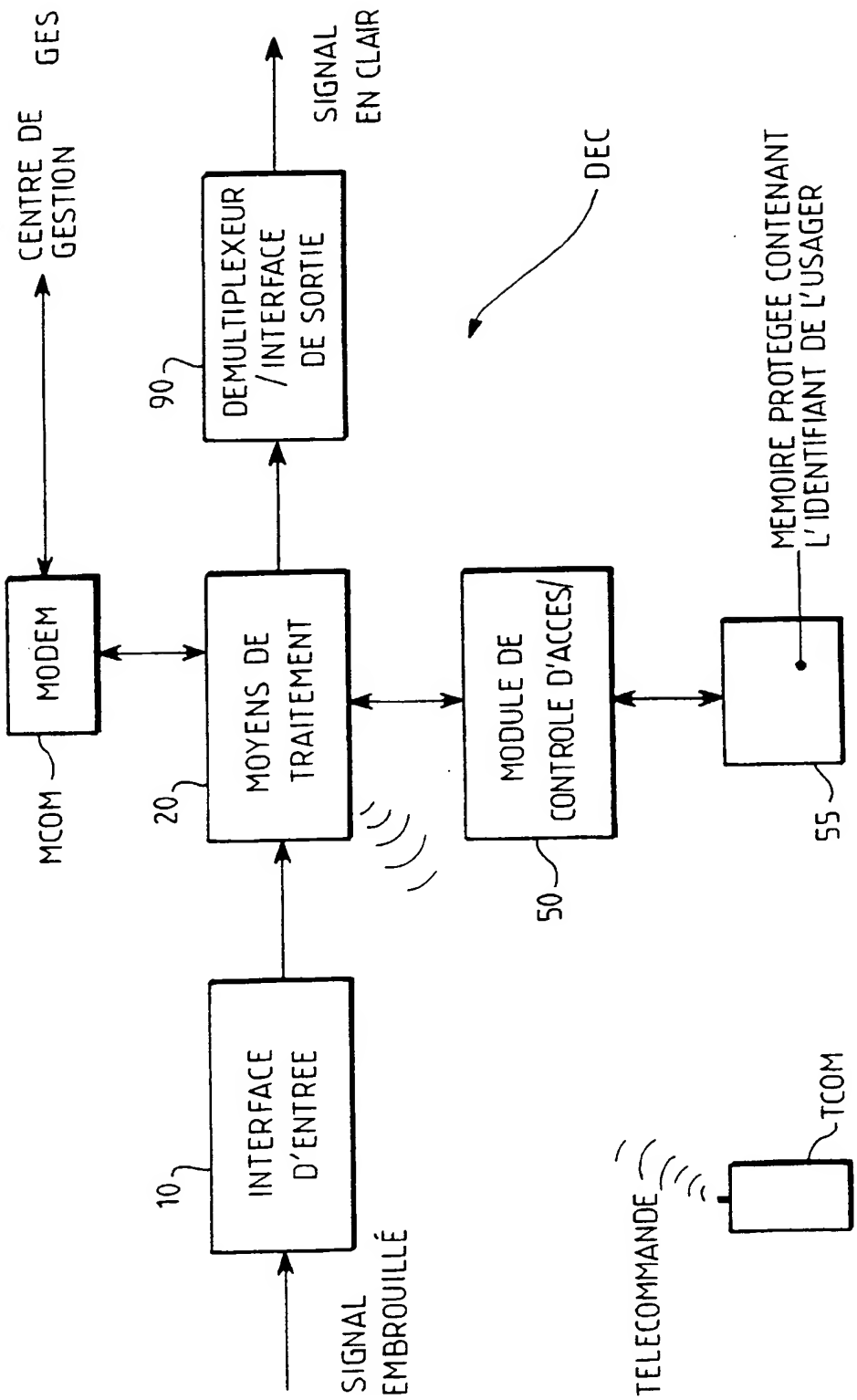

CENTRE DE GESTION
GES
SIGNAL EN CLAIR
DEMULTIPLEXEUR / INTERFACE DE SORTIE
90
DEC
MEMOIRE PROTEGEE CONTENANT L'IDENTIFIANT DE L'USAGER
MODEM
MCOM
MOYENS DE TRAITEMENT
20
MODULE DE CONTROLE D'ACCES
50
55
INTERFACE D'ENTREE
10
TCOM
TELECOMMANDE
SIGNAL EMBROUILLÉ

FIG.1

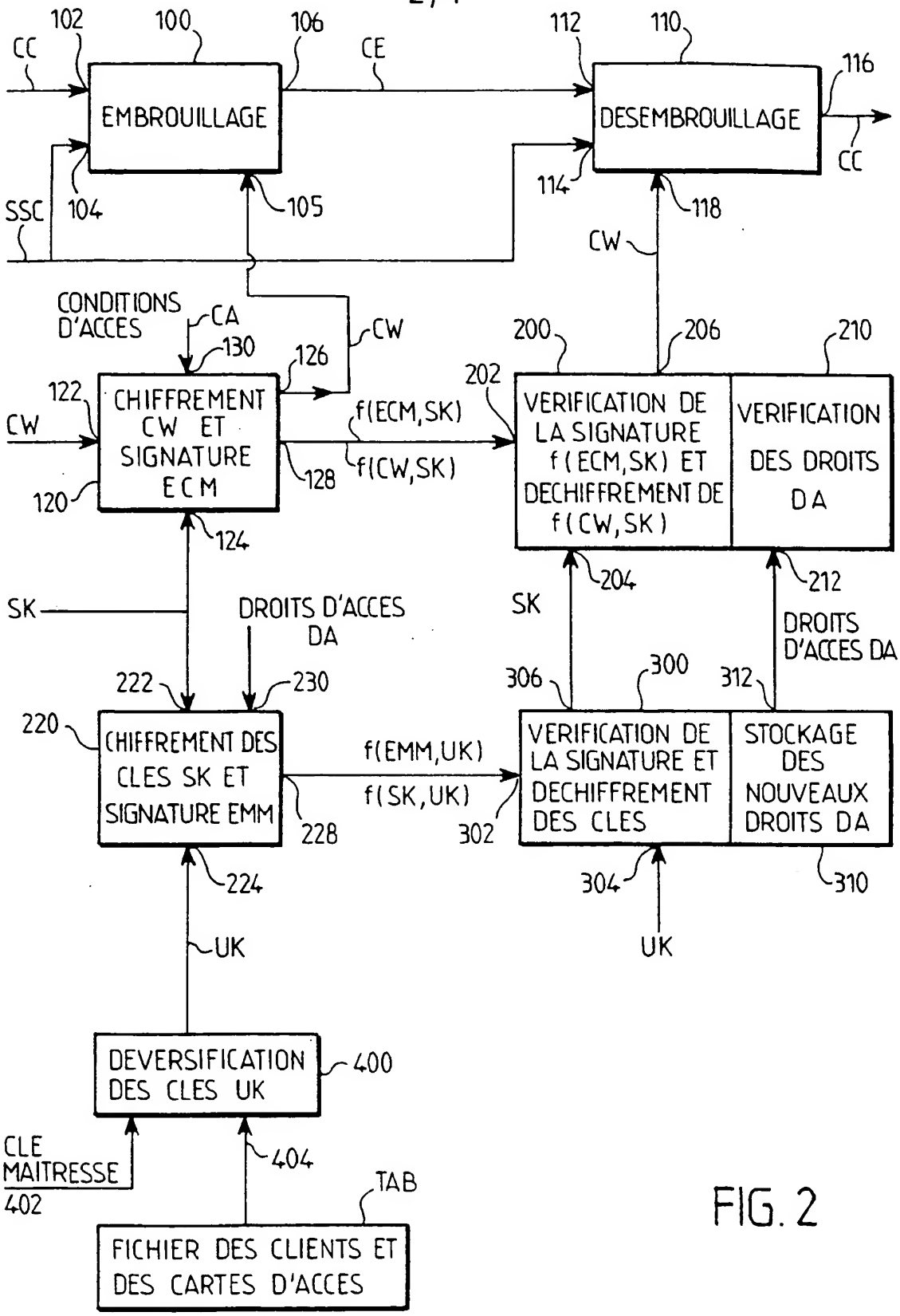

CC
102
100
106
CE
112
110
116
EMBROUILLAGE
DESEMBROUILLAGE
CC
SSC
104
105
114
118
CW
CONDITIONS D'ACCES
CA
130
126
CW
200
206
210
202
122
CW
CHIFFREMENT CW ET SIGNATURE ECM
f(ECM,SK)
f(CW,SK)
VERIFICATION DE LA SIGNATURE f(ECM,SK) ET DECHIFFREMENT DE f(CW,SK)
VERIFICATION DES DROITS DA
120
128
124
SK
DROITS D'ACCES DA
204
212
SK
DROITS D'ACCES DA
222
230
306
300
312
220
CHIFFREMENT DES CLES SK ET SIGNATURE EMM
f(EMM,UK)
f(SK,UK)
VERIFICATION DE LA SIGNATURE ET DECHIFFREMENT DES CLES
STOCKAGE DES NOUVEAUX DROITS DA
228
302
224
304
310
UK
UK
DEVERSIFICATION DES CLES UK
400
CLE MAITRESSE
402
404
TAB
FICHIER DES CLIENTS ET DES CARTES D'ACCES

FIG. 2

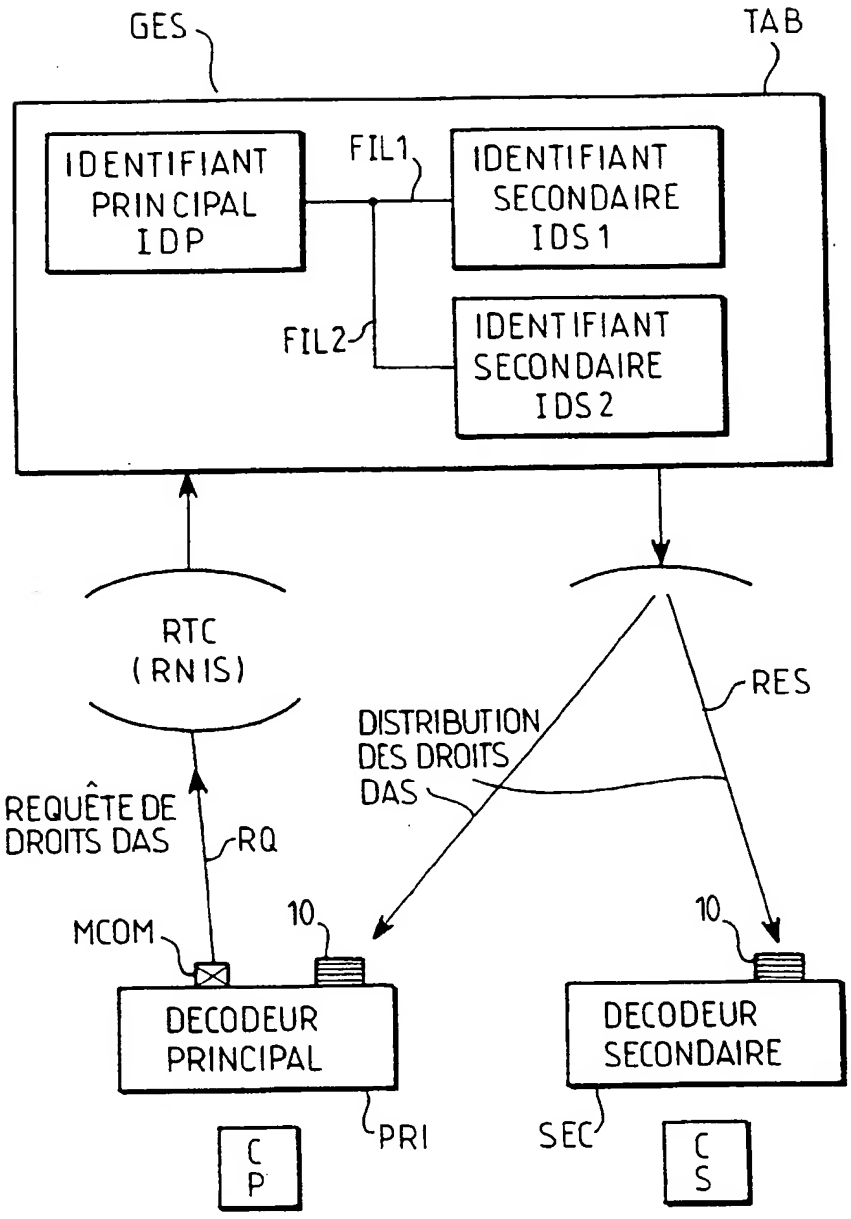

GES
TAB
IDENTIFIANT PRINCIPAL IDP
FIL1
IDENTIFIANT SECONDAIRE IDS1
FIL2
IDENTIFIANT SECONDAIRE IDS2
RTC (RNIS)
RES
DISTRIBUTION DES DROITS DAS
REQUÊTE DE DROITS DAS
RQ
MCOM
10
10
DECODEUR PRINCIPAL
DECODEUR SECONDAIRE
PRI
SEC
C P
C S

FIG.3

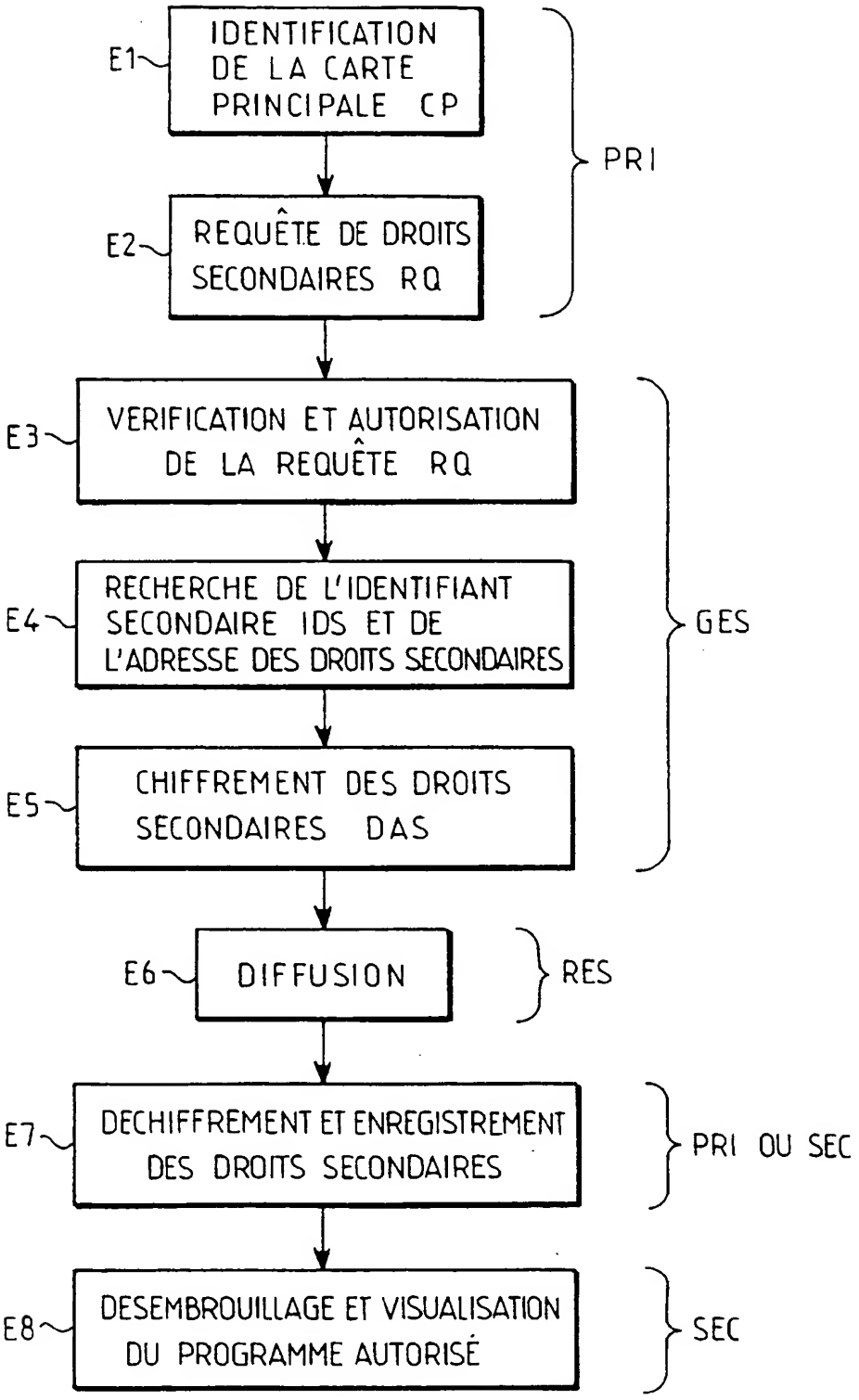

E1
IDENTIFICATION DE LA CARTE PRINCIPALE CP
E2
REQUÊTE DE DROITS SECONDAIRES RQ
PRI
E3
VERIFICATION ET AUTORISATION DE LA REQUÊTE RQ
E4
RECHERCHE DE L'IDENTIFIANT SECONDAIRE IDS ET DE L'ADRESSE DES DROITS SECONDAIRES
E5
CHIFFREMENT DES DROITS SECONDAIRES DAS
GES
E6
DIFFUSION
RES
E7
DECHIFFREMENT ET ENREGISTREMENT DES DROITS SECONDAIRES
PRI OU SEC
E8
DESEMBROUILLAGE ET VISUALISATION DU PROGRAMME AUTORISÉ
SEC

FIG.4

2779599

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 559771
FR 9807026

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	US 5 748 732 A (LE BERRE JACQUES ET AL) 5 mai 1998	1-3
A	* colonne 1, ligne 16 - ligne 25 * * colonne 1, ligne 62 - colonne 2, ligne 11 * * colonne 3, ligne 45 - colonne 4, ligne 23 * * colonne 4, ligne 58 - colonne 5, ligne 7 *	6
X	WO 97 35430 A (NEWS DATACOM LTD ;TSURIA YOSSEF (IL)) 25 septembre 1997	1,4,7
A	* page 9, ligne 6 - ligne 13 * * page 10, ligne 1 - ligne 10 * * page 13, ligne 7 - ligne 22 * * page 14, ligne 25 - page 15, ligne 23 *	5
A	US 4 633 309 A (LI TONY C ET AL) 30 décembre 1986 * colonne 1, ligne 6 - ligne 21 * * colonne 1, ligne 47 - ligne 66 * * colonne 3, ligne 7 - ligne 45 *	1
A	GUILLOU L C ET AL: "ENCIPHERMENT AND CONDITIONAL ACCESS" SMPTE JOURNAL, vol. 103, no. 6, 1 juin 1994, pages 398-406, XP000457575 * page 400, colonne de gauche, alinéa 4 - colonne de droite, alinéa 5 * * page 402, colonne de gauche, alinéa 4 - colonne de droite, alinéa 2 * * page 406, colonne du milieu, alinéa 6 - colonne de droite, alinéa 3 *	1-3

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

H04N

Date d'achèvement de la recherche	Examinateur
16 février 1999	Sindic, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

1